Tips voor veilige(re) digitale communicatie



2024 v 0.1.0

Informatie over digitale veiligheid veroudert snel. Verzeker jezelf ervan dat je een recente versie van dit document gebruikt.

Digitale hygiëne

Het is verbazingwekkend hoeveel je kunt bereiken als je geen roem of erkenning nastreeft.

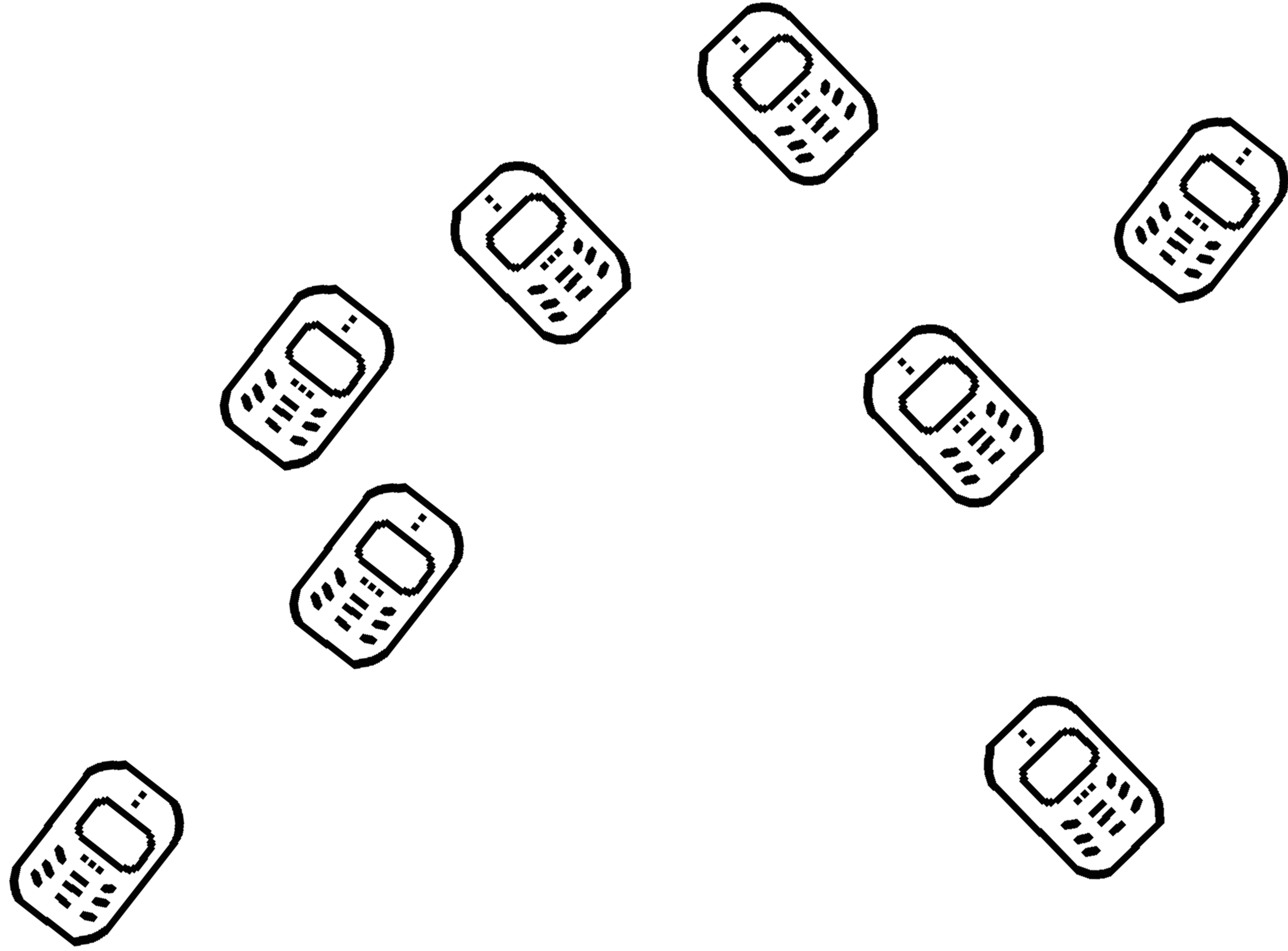
Vermijd opscheppen, roddelen en loslippigheid.

Deel informatie alleen als het écht nodig is.
En deel informatie alleen met mensen die je vertrouwt.

Telefoongebruik

Laat je persoonlijke telefoon zoveel mogelijk thuis. Haal in plaats daarvan een goedkoop (tweedehands) mobieltje dat je als aparte actietelefoon gebruikt. (Het liefst met contant geld betaald.)

Gebruik een kooi van Faraday. Een kooi van Faraday is een soort dikke portemonnee die alle communicatie van en naar je telefoon blokkeert. Je hebt zo'n kooi al voor €30–€50.









Berichten sturen

Gebruik **Session** of **Signal** om berichten te sturen. Op Session en Signal zijn je berichten eind-tot-eind versleuteld. Eind-tot-eind versleuteld houdt in dat alleen jijzelf en de mensen die je een bericht stuurt de inhoud van je bericht kunnen lezen.

Stel verdwijnende berichten in.

🔗 getsession.org

🔗 signal.org

Het internet op

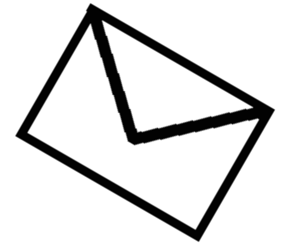
Gebruik de **Tor-browser** om het internet op te gaan. De Tor-browser is een webbrowser die je internetverkeer omleidt via een gratis, wereldwijd netwerk met tussenlagen van vrijwilligers, wat het moeilijker maakt om je internet-activiteit te traceren.

- torproject.org
- protonvpn.com
- mullvad.net

Je kunt ook een virtueel privénetwerk (VPN) gebruiken om met het internet te verbinden, zoals bijvoorbeeld **ProtonVPN** of **MullvadVPN**.

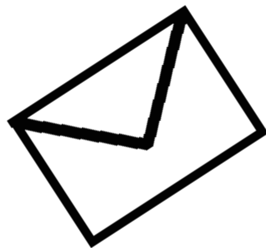
Een VPN biedt je een versleuteld, schijnbaar privé, netwerk — zelfs wanneer je een publieke WiFi-verbinding in een café of hotel gebruikt. Hierdoor kunnen de websites die je bezoekt je minder makkelijk identificeren.

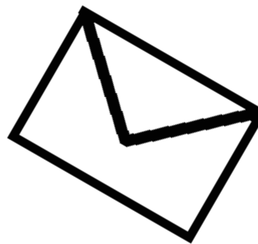
Emailen

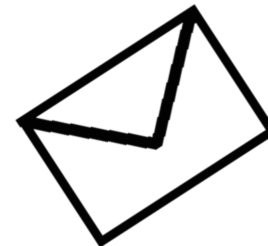


Maak voor acties een apart emailadres aan met **Protonmail**. Protonmail is een aanbieder van eind-tot-eind versleutelde email, wat inhoudt dat alleen jij en de mensen die je mailt de inhoud van je email kunnen lezen.

🔗 proton.me/mail







Sociale media

Gebruik op sociale profielen altijd een actienaam die geen enkele verbinding heeft met jou als persoon.

Geef zo min mogelijk je locatie en persoonlijke gegevens prijs.

Moet je een emailadres of telefoonnummer opgeven om je te registreren? Neem dan een apart protonmail-adres en een aparte SIM-kaart, die je alleen voor dit doeleinde gebruikt.

Foto's en video's

Fotografeer of film alleen als het écht nodig is. Breng mensen niet herkenbaar in beeld.

Heb je gezichten of andere lichaamskenmerken van kameraden gefilmd, zoals tatoeages, moedervlekken, of littekens? Knip deze er dan uit of verdoezel ze, bijvoorbeeld met **ObscuraCam**, of met de 'verdoezel gezichten' optie in Signal.

🔗 guardianproject.info/apps/obscuracam

Verwijder exif-gegevens van bestanden, met bijvoorbeeld **Scrambled Exif** of **ExifCleaner**. Exif-gegevens zijn meta-gegevens zoals locatie, tijd, of camera-instellingen, die je zouden kunnen identificeren.

Vermijd foto's van herkenbare omgevingskenmerken die je locatie zouden kunnen prijsgeven.

🔗 gitlab.com/juanitobananas/scrambled-exif

🔗 exifcleaner.com

Bestanden delen

Moet je beslist documenten met anderen delen? Gebruik dan CryptPad.

Vesleutel je bestanden op CryptPad met wachtwoorden.

Heb je een document na een bepaalde datum niet meer nodig? Stel dan in dat het document zichzelf na die datum vernietigt.

🔗 cryptpad.fr

Ruim op

Heb je foto's, video's, bestanden en berichten die gevoelige informatie bevatten? En heb je ze niet meer nodig? Gooi ze dan weg.







Lijstje ter controle

- [ ] Vermijd loslippigheid
- [ ] Haal een aparte actietelefoon
- [ ] Gebruik versleutelde en verdwijnende berichten
- [ ] Gebruik de Tor-browser of VPN
- [ ] Neem een apart emailadres
- [ ] Blijf anoniem op sociale media
- [ ] Blijf onherkenbaar op foto's
- [ ] Versleutel je bestanden
- [ ] Gooi weg wat je niet nodig hebt